Linearized polynomials over finite fields revisited*

Baofeng Wu†, Zhuojun Liu‡

Abstract

We give new characterizations of the algebra $\mathscr{L}_n(\mathbb{F}_{q^n})$ formed by all linearized polynomials over the finite field $\mathbb{F}_{q^n}$ after briefly surveying some known ones. One isomorphism we construct is between $\mathscr{L}_n(\mathbb{F}_{q^n})$ and the composition algebra $\mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$. The other isomorphism we construct is between $\mathscr{L}_n(\mathbb{F}_{q^n})$ and the so-called Dickson matrix algebra $\mathscr{D}_n(\mathbb{F}_{q^n})$. We also further study the relations between a linearized polynomial and its associated Dickson matrix, generalizing a well-known criterion of Dickson on linearized permutation polynomials. Adjugate polynomial of a linearized polynomial is then introduced, and connections between them are discussed. Both of the new characterizations can bring us more simple approaches to establish a special form of representations of linearized polynomials proposed recently by several authors. Structure of the subalgebra $\mathscr{L}_n(\mathbb{F}_{q^m})$ which are formed by all linearized polynomials over a subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ where $m|n$ are also described.

Keywords Linearized polynomial; Composition algebra; Dickson matrix algebra; Representation.

*Partially supported by National Basic Research Program of China (2011CB302400).

†Key Laboratory of Mathematics Mechanization, AMSS, Chinese Academy of Sciences, Beijing 100190, China. Email: wubaofeng@amss.ac.cn

‡Key Laboratory of Mathematics Mechanization, AMSS, Chinese Academy of Sciences, Beijing 100190, China. Email: zliu@mmrc.iss.ac.cn

1 Introduction

Let $\mathbb{F}_q$ and $\mathbb{F}_{q^n}$ be the finite fields with q and q^n elements respectively, where q is a prime or a prime power. Polynomials over $\mathbb{F}_{q^n}$ of the form

$$L(x) = \sum_{i=0}^{t} a_i x^{q^i},\ t \in \mathbb{N} \tag{1}$$

are often known as linearized polynomials. Such special kinds of polynomials can induce linear transformations of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Considered as maps between finite fields, linearized polynomials are always taken as

$$L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]/(x^{q^n} - x). \tag{2}$$

We denote by $\mathscr{L}(\mathbb{F}_{q^n})$ and $\mathscr{L}_n(\mathbb{F}_{q^n})$ the set of all linearized polynomials in the form (1) and (2) respectively. Equipped with the operations of addition and composition of polynomials in $\mathbb{F}_{q^n}[x]$ and $\mathbb{F}_{q^n}[x]/(x^{q^n} - x)$ respectively, and scalar multiplication by elements in $\mathbb{F}_q$, $\mathscr{L}(\mathbb{F}_{q^n})$ and $\mathscr{L}_n(\mathbb{F}_{q^n})$ both form non-commutative $\mathbb{F}_q$-algebras. We mainly focus on the algebra $\mathscr{L}_n(\mathbb{F}_{q^n})$ in this paper, and use "$\circ$" to denote the multiplication in it. Let $\mathscr{L}_n(\mathbb{F}_{q^m}) \subset \mathscr{L}_n(\mathbb{F}_{q^n})$ be the set of linearized polynomials with coefficients in $\mathbb{F}_{q^m}$, where $\mathbb{F}_{q^m}$ is the subfield of $\mathbb{F}_{q^n}$ with q^m elements (which implies $m|n$). It is clear that $\mathscr{L}_n(\mathbb{F}_{q^m})$ is an $\mathbb{F}_q$-subalgebra of $\mathscr{L}_n(\mathbb{F}_{q^n})$ under the operations mentioned above.

Linearized polynomials were firstly studied by Ore in [14] after his work on the theory of non-commutative polynomials [13]. From [14], we can easily get the $\mathbb{F}_q$-algebra isomorphism

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathbb{F}_{q^n}[x;\sigma]/(x^n - 1),$$

where σ is the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, i.e. $\sigma(x) = x^q$ for $x \in \mathbb{F}_{q^n}$, and $\mathbb{F}_{q^n}[x;\sigma]$ is the so-called skew-polynomial ring. Actually, it is clear that every linear transformation of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can be induced by a linearized polynomial, thus we have

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathscr{M}_n(\mathbb{F}_q),$$

where $\mathscr{M}_n(\mathbb{F}_q)$ is the algebra formed by all $n \times n$ matrices over $\mathbb{F}_q$. This isomorphism was constructed explicitly by Carlitz in [2]. In addition, $\mathscr{L}_n(\mathbb{F}_{q^n})$

is also proved to be isomorphic to $\mathbb{F}_{q^n}[G]$, the so-called semi-linear group algebra, where $G = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. All these results give characterizations of the algebra $\mathscr{L}_n(\mathbb{F}_{q^n})$.

In addition to the known ones, we give two new approaches to characterize the algebra $\mathscr{L}_n(\mathbb{F}_{q^n})$ in this paper. One isomorphism we construct is

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}, \tag{3}$$

where $\mathbb{F}_{q^n}^{\vee}$ is the dual space of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $\mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ is the so-called composition algebra on $\mathbb{F}_{q^n}$. In fact, this is a special case of the composition algebra mentioned in [6]. The other isomorphism we construct is

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathscr{D}_n(\mathbb{F}_{q^n}), \tag{4}$$

where $\mathscr{D}_n(\mathbb{F}_{q^n})$ is an algebra formed by all $n \times n$ matrices over $\mathbb{F}_{q^n}$ of the form

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^q & a_0^q & \dots & a_{n-2}^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & a_0^{q^{n-1}} \end{pmatrix}, \tag{5}$$

which are called Dickson matrices.

A well known result of Dickson indicates that $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathscr{L}_n(\mathbb{F}_{q^n})$ is a linearized permutation polynomial if and only if the Dickson matrix associated to it, i.e. the Dickson matrix with the coefficients a_0, a_1, …, a_{n-1} as entries of the first row, is non-singular [8]. As a matter of fact, a linearized permutation polynomial is just a linearized polynomial of rank n. By the rank of a linearized polynomial, we mean the rank of it as a linear transformation of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, i.e. the dimension of the image space over $\mathbb{F}_q$. We can generalize Dickson's result to that the rank of a linearized polynomial is equal to the rank of the Dickson matrix associated to it. Furthermore, we find that the adjugate matrix of a Dickson matrix is also a Dickson matrix, thus we can define an adjugate polynomial for every linearized polynomial. From this concept, we can derive more properties of linearized polynomials of rank n and $n-1$ respectively.

Recently, it was proved in [10] that for a fixed ordered basis $\{\beta_i\}_{i=0}^{n-1}$, any linearized polynomial $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ of rank k can be represented as

$$L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\beta_i x)\alpha_i$$

or

$$L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\alpha_i' x)\beta_i,$$

where $\{\alpha_i\}_{i=0}^{n-1}$ and $\{\alpha_i'\}_{i=0}^{n-1}$ are two order sets of elements in $\mathbb{F}_{q^n}$ both of rank k over $\mathbb{F}_q$, and "tr" is the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. We notice that that these kinds of representations of linearized polynomials are just direct consequences of the isomorphism (3), thus we rediscover them via a more simple approach. Besides, we can also establish them simply according to the isomorphism (4) and properties of Dickson matrices.

As to the subalgebra $\mathscr{L}_n(\mathbb{F}_{q^m})$, in [15] Ore derived that

$$\mathscr{L}_n(\mathbb{F}_q) \cong \mathbb{F}_q[x]/(x^n - 1),$$

and in [1], Brawley et al. completed the problem. They derived the isomorphism

$$\mathscr{L}_n(\mathbb{F}_{q^m}) \cong \mathscr{M}_m\big(\mathbb{F}_q[x]/(x^t - 1)\big), \tag{6}$$

where $n = mt$ and $\mathscr{M}_m\big(\mathbb{F}_q[x]/(x^t - 1)\big)$ is the algebra formed by all $m \times m$ matrices over the residue ring $\mathbb{F}_q[x]/(x^t - 1)$. We can also give descriptions to the structure of $\mathscr{L}_n(\mathbb{F}_{q^m})$ via constructing isomorphisms between it and subalgebras of $\mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ and $\mathscr{D}_n(\mathbb{F}_{q^n})$ respectively.

In this paper, we revisit linearized polynomials over finite fields and get some new results related to them. The rest of the paper is organized as follows. In Section 2, we briefly survey the known characterizations of the algebra $\mathscr{L}_n(\mathbb{F}_{q^n})$. In Section 3, we propose the composition algebra approach to characterize $\mathscr{L}_n(\mathbb{F}_{q^n})$. In Section 4, we propose the Dickson matrix algebra approach to characterize $\mathscr{L}_n(\mathbb{F}_{q^n})$, and derive more relations between linearized polynomials and their associated Dickson matrices. In Section 5, the trace form representations of linearized polynomials are rediscovered through more simple approaches and studied further. In Section 6, descriptions to the subalgebra $\mathscr{L}_n(\mathbb{F}_{q^m})$ are discussed. Concluding remarks are given in Section 7.

Throughout this paper, we fix an ordered basis $\{\beta_i\}_{i=0}^{n-1}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and denote its dual basis by $\{\beta_i^*\}_{i=0}^{n-1}$, i.e. $\mathrm{tr}(\beta_i\beta_j^*) = \delta_{ij}$, $0 \le i,\ j \le n-1$, where δ is the Kronecker delta. When $\{\beta_i\}_{i=0}^{n-1}$ is a normal basis, we assume $\beta_i = \beta^{q^i}$, $0 \le i \le n-1$, where β is the normal basis generator with dual basis generator β^*. For a set of elements $\{\alpha_i\}_{i=0}^{s}$, we denote by $\mathrm{rk}_{\mathbb{F}_q}\{\alpha_i\}_{i=0}^{s}$ to be its rank over $\mathbb{F}_q$. The rank of a linearized polynomial $L(x)$ and a matrix M are denoted

to be $\operatorname{rk} L$ and $\operatorname{rk} M$ respectively. For a matrix $\left(a_{ij}\right)_{0\le i\le n-1,\,0\le j\le n-1}$ with the (i,j)-th entry a_{ij}, we sometimes use $\left(a_{ij}\right)$ to represent it for simplicity. For example, we always denote the Dickson matrix in (5) by $\left(a_{j-i}^{q^i}\right)$ (subscripts reduced modulo n).

2 Known characterizations of $\mathscr{L}_n(\mathbb{F}_{q^n})$

As mentioned in Section 1, the $\mathbb{F}_q$-algebra $\mathscr{L}_n(\mathbb{F}_{q^n})$ can be characterized through various approaches. For completeness of this paper, we firstly recall the known ones briefly in this part.

2.1 The skew-polynomial ring approach

Let σ be the Frobenius automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\mathbb{F}_{q^n}[x;\sigma]$ be the set of all (skew-)polynomials over $\mathbb{F}_{q^n}$. Define the addition of polynomials in the standard manner and multiplication of polynomials by distribute law and

$$(ax^i)(bx^j) = a\sigma^i(b)x^{i+j} = ab^{q^i}x^{i+j}, \quad a,\ b \in \mathbb{F}_{q^n}.$$

With these operations, $\mathbb{F}_{q^n}[x;\sigma]$ forms a ring called the skew-polynomial ring over $\mathbb{F}_{q^n}$ with automorphism σ. This is a special case of Ore's non-commutative polynomial ring proposed in [13]. It can be proved that $\mathbb{F}_{q^n}[x;\sigma]$ is a principle ideal domain, i.e. a ring with no zero divisors and whose left and right ideals are all principle. $\mathbb{F}_{q^n}[x;\sigma]$ also becomes an $\mathbb{F}_q$-algebra under scalar multiplication of elements in $\mathbb{F}_q$.

Define

$$\begin{array}{rccc} \phi: & \mathbb{F}_{q^n}[x;\sigma] & \longrightarrow & \mathscr{L}(\mathbb{F}_{q^n}) \\ & \displaystyle\sum_{i=0}^{t} a_i x^i & \longmapsto & \displaystyle\sum_{i=0}^{t} a_i x^{q^i} \end{array}$$

Note that $(ax^i)(bx^j) = ab^{q^i}x^{i+j}$ is mapped to $ab^{q^i}x^{q^{i+j}} = (ax^{q^i}) \circ (bx^{q^j})$. The following theorem is straightforward.

Theorem 2.1. *The above map ϕ defines an algebra isomorphism*

$$\mathscr{L}(\mathbb{F}_{q^n}) \cong \mathbb{F}_{q^n}[x;\sigma].$$

It is easy to find that (x^n-1) and $(x^{q^n}-x)$ are two-sided ideals of $\mathbb{F}_{q^n}[x;\sigma]$ and $\mathscr{L}(\mathbb{F}_{q^n})$ respectively, and $\phi(x^n-1)=x^{q^n}-x$, so a map $\bar{\phi}$ between quotient algebras can be induced by ϕ. Hence we have:

Theorem 2.2 ([14])**.**

$$\mathscr{L}_n(\mathbb{F}_{q^n})=\mathscr{L}(\mathbb{F}_{q^n})/(x^{q^n}-x)\cong\mathbb{F}_{q^n}[x;\sigma]/(x^n-1).$$

Remark 2.3. *Since $\mathbb{F}_{q^n}[x;\sigma]$ is a right Euclidean domain, the greatest common right divisor (gcrd) of two skew-polynomials can be computed [13]. It is easy to prove that* $\operatorname{rk} L=n-\deg\operatorname{gcrd}(\phi^{-1}(L(x)),x^n-1)$ *for any $L(x)\in\mathscr{L}_n(\mathbb{F}_{q^n})$ (viewed as an element of $\mathscr{L}(\mathbb{F}_{q^n})$ formally), where the degree of a skew-polynomial $f(x)$, $\deg f$, is defined to be the degree of it as a usual polynomial. This supplies an approach to get rank of a given linearized polynomial. Algorithms for computing gcrd of two skew-polynomials and their complexity can be found in [5]. As a special case, we know that* $\operatorname{rk} L=n-1$ *if and only if* $\deg\operatorname{gcrd}(\phi^{-1}(L(x)),x^n-1)=1$*. This is equivalent to say $L(x)$ is of the form*

$$L(x)=L_1(x)\circ(x^q-ax),$$

where $a\in\left(\mathbb{F}_{q^n}\right)^{q-1}$ and $\deg L_1=(\deg L)/q$ (the degree of a linearized polynomial in $\mathscr{L}_n(\mathbb{F}_{q^n})$ is defined in the usual sense viewing it as a polynomial in $\mathscr{L}(\mathbb{F}_{q^n})$ formally). This will supply an answer to the open problem proposed in [3] to an extent. We will discuss this in detail in Section 3.

2.2 The semi-linear group algebra approach

Let $G=\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)=\langle\sigma\rangle$ be the Galois group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $\mathbb{F}_{q^n}[G]$ be the vector space generated by elements in G over $\mathbb{F}_{q^n}$. Define the multiplication operation in $\mathbb{F}_{q^n}[G]$ by the distribute law and

$$(a\sigma^i)(b\sigma^j)=a\sigma^i(b)\sigma^{i+j}=ab^{q^i}\sigma^{i+j},\quad a,\ b\in\mathbb{F}_{q^n}.$$

With this operation, $\mathbb{F}_{q^n}[G]$ forms a non-commutative ring called the semi-linear group ring over $\mathbb{F}_{q^n}$. It is also an $\mathbb{F}_q$-algebra under scalar multiplication by elements in $\mathbb{F}_q$.

By the definition of the multiplication in $\mathbb{F}_{q^n}[G]$, it is easy to see that the map

$$\mathbb{F}_{q^n}[G]\ \longrightarrow\ \mathscr{L}_n(\mathbb{F}_{q^n})$$

$$\sum_{i=0}^{n-1} a_i\sigma^i \longmapsto \sum_{i=0}^{n-1} a_i x^{q^i}$$

is an algebra homomorphism. By comparing dimensions, we can get

Theorem 2.4 ([11])**.**

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathbb{F}_{q^n}[G].$$

2.3 The matrix algebra approach

Let $\mathscr{M}_n(\mathbb{F}_q)$ be the matrix algebra over $\mathbb{F}_q$ and $\mathrm{End}(\mathbb{F}_{q^n})$ be the algebra of linear transformations of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It is well known that every linear transformation of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can be induced by a linearized polynomial over $\mathbb{F}_{q^n}$. This is because $\mathrm{End}(\mathbb{F}_{q^n})$ is an $\mathbb{F}_q$-vector space, which becomes an $\mathbb{F}_{q^n}$-vector space under the scalar multiplication

$$(aT)(x) = aT(x),\ \forall x \in \mathbb{F}_{q^n}$$

for any $a \in \mathbb{F}_{q^n}$ and $T \in \mathrm{End}(\mathbb{F}_{q^n})$. Note that $\{\sigma^i \in \mathrm{End}(\mathbb{F}_{q^n})|\ 0 \leq i \leq n-1\}$ is linearly independent over $\mathbb{F}_{q^n}$ since if not so, the polynomial $\sum_{i=0}^{n-1} a_i\sigma^i(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ will admit q^n roots for some $a_0, \cdots, a_{n-1} \in \mathbb{F}_{q^n}$ which are not all zero. As $\dim_{\mathbb{F}_q} \mathrm{End}(\mathbb{F}_{q^n}) = n^2$ and $\dim_{\mathbb{F}_q} \mathbb{F}_{q^n} = n$, we have

$$\dim_{\mathbb{F}_{q^n}} \mathrm{End}(\mathbb{F}_{q^n}) = n,$$

which implies that for any $T \in \mathrm{End}(\mathbb{F}_{q^n})$, there exist $a_0, \cdots, a_{n-1} \in \mathbb{F}_{q^n}$ such that $T = \sum_{i=0}^{n-1} a_i\sigma^i$. Define a map

$$\begin{array}{ccc} \mathrm{End}(\mathbb{F}_{q^n}) & \longrightarrow & \mathscr{L}_n(\mathbb{F}_{q^n}) \\ \sum_{i=0}^{n-1} a_i\sigma^i & \longmapsto & \sum_{i=0}^{n-1} a_i x^{q^i}. \end{array}$$

It is easy to find that this map is bijective.

Moreover, it is straightforward to verify that the map defined above is an $\mathbb{F}_q$-algebra isomorphism. From linear algebra we finally get:

Theorem 2.5 ([11])**.**

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathscr{M}_n(\mathbb{F}_q).$$

In [2] Carlitz explicitly constructed the matrix corresponding to a linearized permutation polynomial by fixing a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. However, we find that the matrix corresponding to any linearized polynomial can be explicitly constructed under any fixed basis with the aid of the Dickson matrix associated to the given polynomial. We will talk about this in detail in Section 4.

3 Characterize $\mathscr{L}_n(\mathbb{F}_{q^n})$ via the composition algebra

Let E be a vector space over a field $\mathbb{K}$, and $E^\vee$ be its dual space, i.e. $E^\vee = \mathrm{Hom}_{\mathbb{K}}(E, \mathbb{K})$. Define a multiplication in the tensor space $E^\vee \otimes_{\mathbb{K}} E$ by setting

$$(l_1 \otimes x_1)(l_2 \otimes x_2) = l_1(x_2)l_2 \otimes x_1$$

for any $l_1,\ l_2 \in E^\vee$ and $x_1,\ x_2 \in E$, and expanding it by linearity to the whole space. It is easy to verify that this multiplication makes $E^\vee \otimes_{\mathbb{K}} E$ into an associate (non-commutative) $\mathbb{K}$-algebra called the composition algebra [6].

Consider the map $\Lambda :\ E^\vee \otimes_{\mathbb{K}} E \longrightarrow \mathrm{End}_{\mathbb{K}}(E)$ defined by $\Lambda(l \otimes x)(y) = l(y)x$ for any $y \in E$. It can be verified that Λ is an injective algebra homomorphism. Thus Λ is an algebra isomorphism when E is furthermore of a finite dimension.

Now we let $E = \mathbb{F}_{q^n}$, which is an n-dimensional $\mathbb{F}_q$-vector space, and consider the composition algebra $\mathbb{F}_{q^n}^\vee \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$. Recall the isomorphism between $\mathscr{L}_n(\mathbb{F}_{q^n})$ and $\mathrm{End}(\mathbb{F}_{q^n})$, we get the following theorem straightforwardly from the above discussions.

Theorem 3.1.

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathbb{F}_{q^n}^\vee \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}.$$

In fact, the isomorphism in Theorem 3.1 can be constructed directly. Let $T_\alpha \in \mathbb{F}_{q^n}^\vee$ be the linear function defined by

$$T_\alpha(x) = \mathrm{tr}(\alpha x), \quad \forall x \in \mathbb{F}_{q^n},$$

for any $\alpha \in \mathbb{F}_{q^n}$. As is well known that

$$\mathbb{F}_{q^n}^\vee = \{T_\alpha |\ \alpha \in \mathbb{F}_{q^n}\}$$

(a short proof is like this: define a scalar multiplication by elements in $\mathbb{F}_{q^n}$ as $(\alpha T)(x) = T(\alpha x)$, $\forall x \in \mathbb{F}_{q^n}$, for any $T \in \mathbb{F}_{q^n}^\vee$, which makes $\mathbb{F}_{q^n}^\vee$ into an $\mathbb{F}_{q^n}$-vector space. Its dimension is obviously 1, so the trace function is an $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^n}^\vee$ as a nonzero element of it). Define a map ψ as

$$\begin{aligned} \psi : \ \mathbb{F}_{q^n}^\vee \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} &\longrightarrow \mathscr{L}_n(\mathbb{F}_{q^n}) \\ T_\alpha \otimes \beta &\longmapsto \mathrm{tr}(\alpha x)\beta = \sum_{i=0}^{n-1} \beta \alpha^{q^i} x^{q^i}. \end{aligned} \tag{7}$$

It is easy to see that ψ just defines the isomorphism map we need.

The isomorphism map ψ indicates that every linearized polynomial $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ admits some kind of "trace representation" like $L(x) = \sum_{i=0}^{s} \mathrm{tr}(\omega_i x)\theta_i$ for some ω_i, $\theta_i \in \mathbb{F}_{q^n}$, $0 \le i \le s$, since every element of $\mathbb{F}_{q^n}^\vee \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ is a sum of some single tensors. However, this kind of representation is not unique for $L(x)$. We will talk about this in detail in Section 5.

4 Characterize $\mathscr{L}_n(\mathbb{F}_{q^n})$ via the Dickson matrix algebra and further

As mentioned before, we call a matrix of the form $D_L = \left(a_{j-i}^{q^i}\right) \in \mathscr{M}_n(\mathbb{F}_{q^n})$ a Dickson matrix or a σ-circulant matrix associated to the linearized polynomial $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathscr{L}_n(\mathbb{F}_{q^n})$. Denote by $\mathscr{D}_n(\mathbb{F}_{q^n})$ the set of all $n \times n$ Dickson matrices over $\mathbb{F}_{q^n}$. It can be verified that $\mathscr{D}_n(\mathbb{F}_{q^n})$ forms an $\mathbb{F}_q$-algebra under operations in the standard manner. It is clear that $\mathscr{D}_n(\mathbb{F}_{q^n})$ is an $\mathbb{F}_q$-vector space. To verify that $\mathscr{D}_n(\mathbb{F}_{q^n})$ is a ring, we need only to verify that $\mathscr{D}_n(\mathbb{F}_{q^n})$ is closed under multiplication of matrices as associativity always holds for this multiplication. This can be completed by noting that, for a_i, $b_i \in \mathbb{F}_{q^n}$, $0 \le i \le n-1$,

$$\left(a_{j-i}^{q^i}\right)\left(b_{j-i}^{q^i}\right) = \left(\sum_{k=0}^{n-1} a_{k-i}^{q^i} b_{j-k}^{q^k}\right) = \left(\sum_{k=0}^{n-1} a_k^{q^i} b_{j-i-k}^{q^{k+i}}\right) = \left(c_{j-i}^{q^i}\right) \tag{8}$$

where $c_i = \sum_{k=0}^{n-1} a_k b_{i-k}^{q^k}$, $0 \le i \le n-1$.

As an $\mathbb{F}_q$-algebra, $\mathscr{D}_n(\mathbb{F}_{q^n})$ is an $\mathbb{F}_q$-subalgebra of $\mathscr{M}_n(\mathbb{F}_{q^n})$. However, it is not an $\mathbb{F}_{q^n}$-algebra while $\mathscr{M}_n(\mathbb{F}_{q^n})$ is. Due to its connections to linearized polynomials, we have the $\mathbb{F}_q$-algebra isomorphism in the following theorem.

Theorem 4.1.

$$\mathscr{L}_n(\mathbb{F}_{q^n}) \cong \mathscr{D}_n(\mathbb{F}_{q^n}).$$

Proof. A map from $\mathscr{L}_n(\mathbb{F}_{q^n})$ to $\mathscr{D}_n(\mathbb{F}_{q^n})$ can be constructed straightforwardly as

$$\begin{aligned} \varphi: \ \mathscr{L}_n(\mathbb{F}_{q^n}) &\longrightarrow \mathscr{D}_n(\mathbb{F}_{q^n}) \\ L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} &\longmapsto D_L. \end{aligned}$$

φ is clearly an isomorphism between vector spaces. On the other hand, since

$$\begin{aligned} L_1(x) \circ L_2(x) &= \sum_{i=0}^{n-1} a_i \big(\sum_{j=0}^{n-1} b_j x^{q^j} \big)^{q^i} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} a_i b_j^{q^i} x^{q^{i+j}} \\ &= \sum_{i=0}^{n-1} \big(\sum_{k=0}^{n-1} a_k b_{i-k}^{q^k} \big) x^{q^i} \end{aligned}$$

for $L_1(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, $L_2(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathscr{L}_n(\mathbb{F}_{q^n})$. Hence we have

$$\begin{aligned} \varphi(L_1(x) \circ L_2(x)) &= D_{L_1 \circ L_2} = \left(\big(\sum_{k=0}^{n-1} a_k b_{j-i-k}^{q^k} \big)^{q^i} \right) \\ &= \left(a_{j-i}^{q^i} \right) \left(b_{j-i}^{q^i} \right) \\ &= \varphi(L_1) \varphi(L_2) \end{aligned}$$

form (8). Thus φ is furthermore an algebra isomorphism. □

From Theorem 4.1, we know that $\dim_{\mathbb{F}_q} \mathscr{D}_n(\mathbb{F}_{q^n}) = n^2$. In fact, we can tell more about the isomorphism in Theorem 4.1 by examining the matrix representations of linearized polynomials under a given basis.

Lemma 4.2. *Let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathscr{L}_n(\mathbb{F}_{q^n})$ and $M_L \in \mathscr{M}_n(\mathbb{F}_q)$ be the matrix of the linear transformation induced by $L(x)$ under the basis $\{\beta_i\}_{i=0}^{n-1}$. Then*

$$M_L = \left(\beta_j^{q^i} \right)^{-1} D_L \left(\beta_j^{q^i} \right). \tag{9}$$

Proof. Assume $M_L = \big(m_{ij}\big)$. Since

$$\big(L(\beta_0), \ldots, L(\beta_{n-1})\big) = (\beta_0, \ldots, \beta_{n-1})M_L,$$

we have

$$m_{ij} = \mathrm{tr}(\beta_i^* L(\beta_j)), \quad 0 \le i,\ j \le n-1,$$

i.e.

$$M_L = \big(\mathrm{tr}(\beta_i^* L(\beta_j))\big) = \left(\beta_i^{*q^j}\right)\left(L(\beta_j)^{q^i}\right).$$

Note that

$$L(x)^{q^i} = \big(\sum_{j=0}^{n-1} a_j x^{q^j}\big)^{q^i} = \sum_{j=0}^{n-1} a_{j-i}^{q^i} x^{q^j}$$

for $0 \le i \le n-1$, i.e.

$$\begin{pmatrix} L(x) \\ L(x)^q \\ \vdots \\ L(x)^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1}^q & a_0^q & \ldots & a_{n-2}^q \\ \vdots & \vdots & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \ldots & a_0^{q^{n-1}} \end{pmatrix} \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} = D_L \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix}.$$

Hence

$$\left(L(\beta_j)^{q^i}\right) = D_L \left(\beta_j^{q^i}\right).$$

Besides, it is obvious that $\left(\beta_i^{*q^j}\right) = \left(\beta_j^{q^i}\right)^{-1}$ since

$$\left(\beta_i^{*q^j}\right)\left(\beta_j^{q^i}\right) = \big(\mathrm{tr}(\beta_i^* \beta_j)\big) = I_n,$$

where I_n is the $n \times n$ identity matrix. At last we get

$$M_L = \left(\beta_j^{q^i}\right)^{-1} D_L \left(\beta_j^{q^i}\right).$$

□

Proposition 4.3. *For any $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$, $\mathrm{rk}\, L = \mathrm{rk}\, D_L$ and $\det L = \det D_L$, where $\mathrm{rk}\, L$ and $\det L$ are the rank and determinant, respectively, of the linear transformation induced by $L(x)$.*

Proof. From Lemma 4.2, we can obviously get

$$\det L = \det M_L = \det D_L.$$

Besides, we have $\operatorname{rk} M_L = \operatorname{rk} D_L$ though M_L and D_L are matrices over different fields, since if there exist P, $Q \in GL_n(\mathbb{F}_q)$, where $GL_n(\mathbb{F}_q)$ is the general linear group over $\mathbb{F}_q$, such that $M_L = PEQ$, where

$$E = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \operatorname{rk} M_L \text{ rows} \quad , \tag{10}$$

then

$$D_L = \left(\beta_j^{q^i}\right) PEQ \left(\beta_j^{q^i}\right)^{-1} = RES$$

where R, $S \in GL_n(\mathbb{F}_{q^n})$. □

Proposition 4.3 is a direct generalization of Dickson's well known criterion on linearized permutation polynomials, which concludes that a linearized polynomial is a permutation polynomial if and only if the Dickson matrix associated to it is non-singular [8, Chap. 7]. It is also implied by Proposition 4.3 that the determinant of any Dickson matrix over $\mathbb{F}_{q^n}$ is an element of $\mathbb{F}_q$. A direct consequence of this when $q = 2$ is as follows.

Corollary 4.4. *Let $L(x) \in \mathscr{L}_n(\mathbb{F}_{2^n})$ be a linearized permutation polynomial. Then* $\det L = 1$.

Recall the isomorphism in Theorem 4.1 and Theorem 2.5, we are clear that the set of all non-singular Dickson matrices form a group, which is isomorphic to the general linear group $GL_n(\mathbb{F}_q)$. A direct consequence is that the inverse of an non-singular Dickson matrix is also of the Dickson type. For D_L associated to a linearized permutation polynomial $L(x)$, D_L^{-1} is just the Dickson matrix associated to $L^{-1}(x)$, the composition inverse of $L(x)$. This supplies us a method to compute inverse polynomials of linearized permutation polynomials.

Theorem 4.5. *Let* $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathscr{L}_n(\mathbb{F}_{q^n})$ *be a linearized permutation polynomial and* D_L *be its associated Dickson matrix. Assume* $\bar{a}_i$ *is the* $(i,0)$*-th cofactor of* D_L*,* $0 \le i \le n-1$*. Then* $\det L = \sum_{i=0}^{n-1} a_{n-i}^{q^i} \bar{a}_i$ *and*

$$L^{-1}(x) = \frac{1}{\det L} \sum_{i=0}^{n-1} \bar{a}_i x^{q^i} = \big(\sum_{i=0}^{n-1} \bar{a}_i x^{q^i}\big) \circ \big(\frac{x}{\det L}\big).$$

Proof. The statement on $\det L$ is obvious. Besides, $\bar{a}_0$, $\bar{a}_1$, ..., $\bar{a}_{n-1}$ are entries of the first row of the adjugate matrix $D_L^\star$ of D_L. From linear algebra, we know that

$$D_L^{-1} = \frac{1}{\det L} D_L^\star,$$

which is the Dickson matrix associated to $L^{-1}(x)$. Since $\det L \in \mathbb{F}_q$, the result is straightforward. □

From Theorem 4.5, we know that the main task is to compute cofactors of elements of the first column of a Dickson matrix as its determinant can be obtained by Laplacian expansion afterwards in computing inverse polynomial of a linearized permutation polynomial. The proof of Theorem 4.5 also implies that the adjugate matrix of a non-singular Dickson matrix is also of the Dickson type. In fact, this holds for any Dickson matrices.

Lemma 4.6. *Let* $D \in \mathscr{D}_n(\mathbb{F}_{q^n})$*. Then there exist two sets of elements* $\{\alpha'_i\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$ *and* $\{\alpha_i\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$ *such that*

$$D = \left(\beta_j^{q^i}\right)\left(\alpha_i'^{q^j}\right) = \left(\alpha_j^{q^i}\right)\left(\beta_i^{q^j}\right).$$

Proof. Assume $D = D_L$ is the Dickson matrix associated to a linearized polynomial $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ and M_L is the matrix of the linear transformation induced by $L(x)$ under the basis $\{\beta_i\}_{i=0}^{n-1}$. From Lemma 4.2, we have

$$D = \left(\beta_j^{q^i}\right) M_L \left(\beta_j^{q^i}\right)^{-1} = \left(\beta_j^{q^i}\right)\left(\alpha_i'^{q^j}\right)$$

where $(\alpha'_0, \ldots, \alpha'_{n-1}) = (\beta_0^*, \ldots, \beta_{n-1}^*) M_L^\tau$. The other part of the lemma can be got in the same way by replacing $\{\beta_i\}_{i=0}^{n-1}$ by $\{\beta_i^*\}_{i=0}^{n-1}$ in Lemma 4.2. □

Remark 4.7. *From [8, Lemma 3.51], we know that the determinant of a Dickson matrix D can be represented in the form*

$$\det D = \alpha_0\beta_0 \prod_{i=0}^{n-2} \prod_{c_0,\ldots,c_i\in\mathbb{F}_q} \big(\alpha_{i+1} - \sum_{j=1}^{i} c_j\alpha_j\big)\big(\beta_{i+1} - \sum_{j=1}^{i} c_j\beta_j\big).$$

Besides, it is obvious from Lemma 4.6 that

$$\mathrm{rk}\, D = \mathrm{rk}\, \left(\alpha_j^{'q^i}\right) = \mathrm{rk}\, \left(\alpha_j^{q^i}\right),$$

where the notations are the same as in Lemma 4.6.

Lemma 4.8. *Let $\{\alpha_i\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$. Let $\tilde{\alpha}_i$ be the $(0,i)$-th cofactor of the matrix $\left(\alpha_j^{q^i}\right)$, $0 \le i \le n-1$. Then*

$$\left(\alpha_j^{q^i}\right)^{\star} = \left(\tilde{\alpha}_i^{q^j}\right) S,$$

where $S = \mathrm{diag}\big((-1)^0, (-1)^{n+1}, (-1)^{2(n+1)}, \ldots, (-1)^{(n-1)(n+1)}\big)$, i.e. $S = I_n$ when n is odd and $S = \mathrm{diag}(1,-1,1,-1,\ldots,1,-1)$ when n is even.

Proof. Let $A = \left(\alpha_j^{q^i}\right)$ and A_{ij} be the (i,j)-th cofactor of A, $0 \le i,\ j \le n-1$. We need only to prove $A_{ji} = (-1)^{j(n+1)}\tilde{\alpha}_i^{q^j}$ for any $0 \le i,\ j \le n-1$. This can be completed by noting that

$$\begin{aligned}
\tilde{\alpha}_i^{q^j} &= (-1)^{i+2}\left(\det \begin{pmatrix} \alpha_0^q & \cdots & \alpha_{i-1}^q & \alpha_{i+1}^q & \cdots & \alpha_{n-1}^q \\ \alpha_0^{q^2} & \cdots & \alpha_{i-1}^{q^2} & \alpha_{i+1}^{q^2} & \cdots & \alpha_{n-1}^{q^2} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_0^{q^{n-1}} & \cdots & \alpha_{i-1}^{q^{n-1}} & \alpha_{i+1}^{q^{n-1}} & \cdots & \alpha_{n-1}^{q^{n-1}} \end{pmatrix}\right)^{q^j} \\
&= (-1)^{i+2}\det \begin{pmatrix} \alpha_0^{q^{j+1}} & \cdots & \alpha_{i-1}^{q^{j+1}} & \alpha_{i+1}^{q^{j+1}} & \cdots & \alpha_{n-1}^{q^{j+1}} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_0^{q^{n-1}} & \cdots & \alpha_{i-1}^{q^{n-1}} & \alpha_{i+1}^{q^{n-1}} & \cdots & \alpha_{n-1}^{q^{n-1}} \\ \alpha_0 & \cdots & \alpha_{i-1} & \alpha_{i+1} & \cdots & \alpha_{n-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ \alpha_0^{q^{j-1}} & \cdots & \alpha_{i-1}^{q^{j-1}} & \alpha_{i+1}^{q^{j-1}} & \cdots & \alpha_{n-1}^{q^{j-1}} \end{pmatrix}
\end{aligned}$$

$$
\begin{aligned}
&= (-1)^{i+2}(-1)^{j(n-j-1)}\det \begin{pmatrix}
\alpha_0 & \cdots & \alpha_{i-1} & \alpha_{i+1} & \cdots & \alpha_{n-1} \\
\vdots & & \vdots & \vdots & & \vdots \\
\alpha_0^{q^{j-1}} & \cdots & \alpha_{i-1}^{q^{j-1}} & \alpha_{i+1}^{q^{j-1}} & \cdots & \alpha_{n-1}^{q^{j-1}} \\
\alpha_0^{q^{j+1}} & \cdots & \alpha_{i-1}^{q^{j+1}} & \alpha_{i+1}^{q^{j+1}} & \cdots & \alpha_{n-1}^{q^{j+1}} \\
\vdots & & \vdots & \vdots & & \vdots \\
\alpha_0^{q^{n-1}} & \cdots & \alpha_{i-1}^{q^{n-1}} & \alpha_{i+1}^{q^{n-1}} & \cdots & \alpha_{n-1}^{q^{n-1}}
\end{pmatrix} \\
&= (-1)^{j(n+1)}A_{ji},
\end{aligned}
$$

since $(-1)^{i+2}(-1)^{j(n-j-1)} = (-1)^{j(n+1)+(i+1)+(j+1)}$. □

Corollary 4.9. *Notations as in Lemma 4.8. If $\{\alpha_i\}_{i=0}^{n-1}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then $\{\tilde{\alpha}_i\}_{i=0}^{n-1}$ is also a basis.*

Proof. From [8, Lemma 3.51], we know that when $\{\alpha_i\}_{i=0}^{n-1}$ is a basis, $\left(\alpha_j^{q^i}\right)$, and consequently $\left(\alpha_j^{q^i}\right)^\star$, is non-singular. Hence $\left(\tilde{\alpha}_i^{q^j}\right)$ is non-singular from Lemma 4.8, which implies that $\{\tilde{\alpha}_i\}_{i=0}^{n-1}$ is a basis using [8, Lemma 3.51] again. □

Lemma 4.10. *Let $D \in \mathscr{D}_n(\mathbb{F}_{q^n})$. Then $SDS \in \mathscr{D}_n(\mathbb{F}_{q^n})$, where S is the matrix defined in Lemma 4.8.*

Proof. We only need to consider the case that n is even. Assume D is a Dickson matrix with entries of the first row $a_0,\ a_1, \ldots, a_{n-1}$. Then it can be verified that SDS is a Dickson matrix with entries of the first row $a_0,\ -a_1,\ a_2,\ -a_3, \ldots, a_{n-2},\ -a_{n-1}$. □

The following lemma is well known in linear algebra.

Lemma 4.11. *Let $N,\ N_1,\ N_2 \in \mathscr{M}_n(\mathbb{K})$, where $\mathbb{K}$ is a field. Then $N^{\tau\star} = N^{\star\tau}$, $(N_1N_2)^\star = N_2^\star N_1^\star$.*

Theorem 4.12. *Let $D \in \mathscr{D}_n(\mathbb{F}_{q^n})$. Then $D^\star \in \mathscr{D}_n(\mathbb{F}_{q^n})$.*

Proof. From Lemma 4.6, we can assume $D = \left(\beta_j^{q^i}\right)\left(\alpha_i^{q^j}\right)$ for a set of elements $\{\alpha_i\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$. Then

$$
D^\star = \left(\alpha_i^{q^j}\right)^\star \left(\beta_j^{q^i}\right)^\star
$$

$$
\begin{aligned}
&= (\left(\tilde{\alpha}_i^{q^j}\right) S)^\tau (\left(\tilde{\beta}_i^{q^j}\right) S) \\
&= S\left(\tilde{\alpha}_j^{q^i}\right)\left(\tilde{\beta}_i^{q^j}\right) S
\end{aligned}
$$

from Lemma 4.8 and Lemma 4.11, where $\tilde{\alpha}_i$ and $\tilde{\beta}_i$ are the $(0,i)$-th cofactors of the matrices $\left(\alpha_j^{q^i}\right)$ and $\left(\beta_j^{q^i}\right)$ respectively, $0 \le i \le n-1$. Hence $D^\star \in \mathscr{D}_n(\mathbb{F}_{q^n})$ from Corollary 4.9, Lemma 4.6 and Lemma 4.10. □

Base on Theorem 4.12, we introduce the following definition.

Definition 4.13. *Let $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$. The adjugate polynomial $L^\star(x)$ of $L(x)$ is defined to be the linearized polynomial associated to $D_L^\star$.*

In fact, the coefficients of $L^\star(x)$ are just cofactors of elements of the first column of D_L. Hence Definition 4.13 is only meaningful for $L(x)$ with $\operatorname{rk} L \ge n-1$ since $D_L^\star = 0$ in other cases. From the fact that $D_L D_L^\star = D_L^\star D_L = (\det D_L) I_n$, we have

$$
L(x) \circ L^\star(x) = L^\star(x) \circ L(x) = (\det L)x. \tag{11}
$$

The case $\operatorname{rk} L = n$ has already been discussed in Theorem 4.5 which indicates that $L^{-1}(x) = \dfrac{1}{\det L} L^\star(x)$. When $\operatorname{rk} L = n-1$, we have the following property.

Proposition 4.14. *Assume* $\operatorname{rk} L = n-1$. *Then* $\operatorname{rk} L^\star = 1$. *Furthermore,*

$$
\ker L^\star = \operatorname{Im} L, \ \operatorname{Im} L^\star = \ker L,
$$

where ker *and* Im *represent kernels and images respectively of linearized polynomials.*

Proof. From linear algebra we know that $\operatorname{rk} D_L^\star = 1$ when $\operatorname{rk} D_L = n-1$ [12], which implies $\operatorname{rk} L^\star = 1$. Furthermore, we have $L(x) \circ L^\star(x) = L^\star(x) \circ L(x) = 0$ since $\det L = 0$. Thus $\operatorname{Im} L^\star \subseteq \ker L$ and $\operatorname{Im} L \subseteq \ker L^\star$. By comparing dimensions, we know that $\operatorname{Im} L^\star = \ker L$ and $\ker L^\star = \operatorname{Im} L$. □

Proposition 4.14 gives characterizations of linearized polynomials with 1-dimensional kernels. For $L(x)$ with $\operatorname{rk} L = n-1$, $\ker L = \gamma \cdot \mathbb{F}_q$ for some $\gamma \in \mathbb{F}_{q^n}^*$ and $\operatorname{Im} L = \mathcal{H}_\delta$ for some $\delta \in \mathbb{F}_{q^n}^*$, where $\mathcal{H}_\delta = \{x \in \mathbb{F}_{q^n} | \operatorname{tr}(\delta x) = 0\}$ is a hyperplane in $\mathbb{F}_{q^n}$. δ can be obtained by computing $L^\star(x)$.

Example 4.15. *Let* $L(x) = x^q - \gamma^{q-1}x \in \mathscr{L}_n(\mathbb{F}_{q^n})$, $\gamma \in \mathbb{F}_{q^n}^*$. *It is obvious that* $\ker L = \gamma \cdot \mathbb{F}_q$. *Besides, it is easy to get*

$$L^\star(x) = (-1)^{n-1}\gamma \mathrm{tr}\big(\frac{x}{\gamma^q}\big),$$

since the $(i,0)$*-th cofactor of the matrix*

$$D_L = \begin{pmatrix} -\gamma^{q-1} & 1 & & & \\ & -\gamma^{(q-1)q} & 1 & & \\ & & \ddots & \ddots & \\ & & -\gamma^{(q-1)q^{n-2}} & 1 \\ 1 & & & -\gamma^{(q-1)q^{n-1}} \end{pmatrix}$$

is $(-1)^{n-1}\gamma^{1-q^{i+1}}$, $0 \le i \le n-1$. *Hence* $\mathrm{Im}\, L = \mathcal{H}_{1/\gamma^q}$.

Generally, we know from Remark 2.3 that for $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ of degree q^d, $0 \le d \le n-1$, with $\mathrm{rk}\, L = n-1$ and $\ker L = \gamma_0 \cdot \mathbb{F}_q$ for some $\gamma_0 \in \mathbb{F}_{q^n}^*$, there exists $L_1(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ of degree q^{d-1} such that

$$L(x) = L_1(x) \circ \left(x^q - \gamma_0^{q-1}x\right).$$

It is clear that $\mathrm{rk}\, L_1 \ge n-1$ and when $\mathrm{rk}\, L_1 = n-1$,

$$\mathrm{Im}\,(x^q - \gamma_0^{q-1}x) \cap \ker L_1 = \{0\}.$$

Assume $\mathrm{rk}\, L_1 = n-1$ and $\ker L_1 = \gamma_1 \cdot \mathbb{F}_q$, $\gamma_1 \in \mathbb{F}_{q^n}^*$. From Example 4.15 we need $\gamma_1 \notin \mathcal{H}_{1/\gamma_0^q}$. Inductively, we finally know that there exist $\gamma_1, \gamma_2, \ldots, \gamma_{r-1} \in \mathbb{F}_{q^n}^*$ for some $r \le d$, satisfying that $\gamma_i \notin \mathcal{H}_{1/\gamma_{i-1}^q}$ (i.e. $\mathrm{tr}(\frac{\gamma_i}{\gamma_{i-1}^q}) \ne 0$) for $1 \le i \le r-1$, and $L_r(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ of degree q^{d-r} which is a linearized permutation polynomial, such that

$$L(x) = L_r(x) \circ \left(x^q - \gamma_{r-1}^{q-1}x\right) \circ \cdots \circ \left(x^q - \gamma_1^{q-1}x\right) \circ \left(x^q - \gamma_0^{q-1}x\right).$$

This can provide an answer to the open problem proposed in [3] to an extent. By Lemma 4.11 and Example 4.15, we have

$$\begin{aligned} L^\star(x) &= \left(x^q - \gamma_0^{q-1}x\right)^\star \circ \left(x^q - \gamma_1^{q-1}x\right)^\star \circ \cdots \circ \left(x^q - \gamma_{r-1}^{q-1}x\right)^\star \circ L_r^\star(x) \\ &= \left[(-1)^{n-1}\gamma_0 \mathrm{tr}\big(\frac{x}{\gamma_0^q}\big)\right] \circ \left[(-1)^{n-1}\gamma_1 \mathrm{tr}\big(\frac{x}{\gamma_1^q}\big)\right] \circ \cdots \end{aligned}$$

$$\circ \left[(-1)^{n-1}\gamma_{r-1}\mathrm{tr}\big(\frac{x}{\gamma_{r-1}^q}\big)\right] \circ L_r^\star(x)$$

$$= \quad (-1)^{r(n-1)}\gamma_0\mathrm{tr}\big(\frac{\gamma_1}{\gamma_0^q}\big)\mathrm{tr}\big(\frac{\gamma_2}{\gamma_1^q}\big)\cdots\mathrm{tr}\big(\frac{\gamma_{r-1}}{\gamma_{r-2}^q}\big)\mathrm{tr}\big(\frac{L_r^\star(x)}{\gamma_{r-1}^q}\big).$$

5 Representations of linearized polynomials

Generally we represent a linearized polynomial by giving its coefficients as a polynomial. Only recently, a new kind of representation was proposed in [18, 17, 10].

Theorem 5.1 ([10]). *Let $L(x) \in \mathscr{L}_n(\mathbb{F}_{q^n})$ be a linearized polynomial of rank k, where k is an integer, $0 \le k \le n$. Then*
(1) there exists a uniquely determined ordered set $\{\alpha_i'\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$ of rank k such that $L(x)$ can be represented as

$$L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\alpha_i' x)\beta_i;$$

(2) there exists a uniquely determined ordered set $\{\alpha_i\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$ of rank k such that $L(x)$ can be represented as

$$L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\beta_i x)\alpha_i;$$

(3) there exist two sets of elements $\{\omega_i\}_{i=0}^{k-1} \subseteq \mathbb{F}_{q^n}$ and $\{\theta_i\}_{i=0}^{k-1} \subseteq \mathbb{F}_{q^n}$ both of rank k such that $L(x)$ can be represented as

$$L(x) = \sum_{i=0}^{k-1} \mathrm{tr}(\omega_i x)\theta_i.$$

This kind of "trace representations" for linearized polynomials was firstly motivated by K. Zhou in [18] and made clear by P.Z. Yuan et al. in [17] for linearized permutation polynomials. Theorem 5.1 was proved by S. Ling and L.J. Qu in [10], solving an open problem proposed in [3] asking for linearized polynomials of rank $n-1$.

In the following, we reestablish Theorem 5.1 via the isomorphism we have constructed in Theorem 3.1 and Theorem 4.1. We will find that both approaches are more simple than that in [10]. Moreover, we can make the reason for the existence of such kind of representations for linearized polynomials clear. Besides, we will talk further about this kind of representations.

5.1 Composition algebra approach to Theorem 5.1

To obtain Theorem 5.1 from Theorem 3.1, we firstly recall the definition of tensor ranks of elements in a tensor space.

Definition 5.2. *Let $V = \bigotimes_{i=1}^{r} V_i$, where V_i, $1 \leq i \leq r$, are all vector spaces over a field $\mathbb{K}$. For any $T \in V$, the tensor rank of it, denoted by $\operatorname{trk} T$, is defined to be*

$$\operatorname{trk} T = \min\{k \in \mathbb{N} | \, \exists v_{ji} \in V_j, \ 1 \leq j \leq r, \ 1 \leq i \leq k, \ s.t. \ T = \sum_{i=1}^{k} v_{1i} \otimes \cdots \otimes v_{ri}\}.$$

Now considering the tensor space $\mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$, we have the following lemma.

Lemma 5.3. *For any $T \in \mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$,*

$$\operatorname{trk} T = \operatorname{rk} \psi(T),$$

where ψ is the map defined in (7) in Section 3.

Proof. Assume $\operatorname{trk} T = k$ for some positive integer k, then there exist two sets of elements $\{\omega_i\}_{i=0}^{k-1} \subseteq \mathbb{F}_{q^n}$ and $\{\gamma_i\}_{i=0}^{k-1} \subseteq \mathbb{F}_{q^n}$ such that

$$T = \sum_{i=0}^{k-1} T_{\omega_i} \otimes \gamma_i.$$

Firstly we prove that $\operatorname{rk}_{\mathbb{F}_q}\{\omega_i\}_{i=0}^{k-1} = \operatorname{rk}_{\mathbb{F}_q}\{\gamma_i\}_{i=0}^{k-1} = k$. If not so, say $\operatorname{rk}_{\mathbb{F}_q}\{\gamma_i\}_{i=0}^{k-1} = r < k$, we have $\gamma_{k-1} = \sum_{i=0}^{k-2} c_i \gamma_i$ for some $c_i \in \mathbb{F}_q$, $0 \leq i \leq k-2$, without loss of generality. Then

$$T = \sum_{i=0}^{k-2} T_{\omega_i} \otimes \gamma_i + T_{\omega_{k-1}} \otimes \sum_{i=0}^{k-2} c_i \gamma_i$$

$$
\begin{aligned}
&= \sum_{i=0}^{k-2} (T_{\omega_i} + c_i T_{\omega_{k-1}}) \otimes \gamma_i \\
&= \sum_{i=0}^{k-2} T_{\omega_i + c_i \omega_{k-1}} \otimes \gamma_i,
\end{aligned}
$$

which contradicts the assumption that $\mathrm{trk}\, T = k$ from the definition of tensor rank. A similar contradiction can be derived if $\mathrm{rk}_{\mathbb{F}_q}\{\omega_i\}_{i=0}^{k-1} < k$.

Now we extend $\{\omega_i\}_{i=0}^{k-1}$ to be a basis $\{\omega_i\}_{i=0}^{n-1}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with dual basis $\{\omega_i^*\}_{i=0}^{n-1}$. Consider the set of elements $\{\psi(T)(\omega_i^*)\}_{i=0}^{n-1}$ in $\mathbb{F}_{q^n}$, which equals $\{\gamma_i\}_{i=0}^{k-1} \cup \{0\}$ since

$$
\psi(T)(\omega_i^*) = \sum_{j=0}^{k-1} \mathrm{tr}(\omega_j \omega_i^*)\gamma_j = \begin{cases} \gamma_i & \text{if } 0 \le i \le k-1 \\ 0 & \text{if } k \le i \le n-1 \end{cases},
$$

we get that $\mathrm{rk}\, \psi(T) = \mathrm{rk}_{\mathbb{F}_q}\{\gamma_i\}_{i=0}^{k-1} = k$. □

From the comments at the end of Section 3 and Lemma 5.3, we get Theorem 5.1(3) directly. We remark that Theorem 5.1(1) and 5.1(2) are both direct consequences of Theorem 5.1(3). For example, to get 5.1(2) from 5.1(3), we assume

$$
(\omega_0, \ldots, \omega_{k-1}) = (\beta_0, \ldots, \beta_{n-1})M,
$$

where M is an $n \times k$ matrix over $\mathbb{F}_q$ with (i,j)-th entry m_{ij}, $0 \le i \le n-1$, $0 \le j \le k-1$, which is of full column rank. Then

$$
\begin{aligned}
L(x) &= \sum_{i=0}^{k-1} \mathrm{tr}(\omega_i x)\theta_i \\
&= \sum_{i=0}^{k-1} \mathrm{tr}\Big(\sum_{j=0}^{n-1} m_{ji}\beta_j x \Big)\theta_i \\
&= \sum_{j=0}^{n-1} \mathrm{tr}(\beta_j x)\Big(\sum_{i=0}^{k-1} m_{ji}\theta_i \Big) \\
&= \sum_{j=0}^{n-1} \mathrm{tr}(\beta_j x)\alpha_j,
\end{aligned}
$$

where

$$(\alpha_0, \ldots, \alpha_{n-1}) = (\theta_0, \ldots, \theta_{k-1})M^\tau.$$

It is clear that $\mathrm{rk}_{\mathbb{F}_q}\{\alpha_i\}_{i=0}^{n-1} = k$. The uniqueness of $\{\alpha_i\}_{i=0}^{n-1}$ can also be easily checked.

In fact, S. Ling and L.J. Qu proved Theorem 5.1(1) and 5.1(2) firstly and 5.1(3) based on them in [10]. Our approach seem more simple to obtain the same result. Besides, we find that it is just due to Theorem 3.1 and the fact that every element in a tensor space can be represented as a sum of single tensors, that there exist "trace representations" for linearized polynomials.

5.2 Dickson matrix algebra approach to Theorem 5.1

We firstly propose the following proposition, which is a direct generalization of Lemma 3.51 in [8].

Proposition 5.4. *Let $k \in \mathbb{N}$ and $\{\alpha_0, \ldots, \alpha_{k-1}\} \subseteq \mathbb{F}_{q^n}$. Then*

$$\mathrm{rk}_{\mathbb{F}_q}\{\alpha_0, \ldots, \alpha_{k-1}\} = \mathrm{rk}\,\Delta(\alpha_0, \ldots, \alpha_{k-1}),$$

where $\Delta(\alpha_0, \ldots, \alpha_{k-1}) = \left(\alpha_j^{q^i}\right)_{0\le i\le k-1,\, 0\le j\le k-1}$.

Proof. It is clear that $\mathrm{rk}_{\mathbb{F}_q}\{\alpha_0, \ldots, \alpha_{k-1}\} \ge \mathrm{rk}\,\Delta(\alpha_0, \ldots, \alpha_{k-1})$. Assume $\mathrm{rk}_{\mathbb{F}_q}\{\alpha_0, \ldots, \alpha_{k-1}\} = r > \mathrm{rk}\,\Delta(\alpha_0, \ldots, \alpha_{k-1}) = r-1$, and

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{r-2} \\ \alpha_0^q & \alpha_1^q & \ldots & \alpha_{r-2}^q \\ \vdots & \vdots & & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \ldots & \alpha_{r-2}^{q^{k-1}} \end{pmatrix}$$

is a submatrix of $\Delta(\alpha_0, \ldots, \alpha_{k-1})$ with full column rank, without loss of generality. Then for any $(c_0, \ldots, c_{r-2}) \in \mathbb{F}_q^{r-1}\backslash\{\mathbf{0}\}$,

$$\sum_{i=0}^{r-2} c_i \begin{pmatrix} \alpha_i \\ \alpha_i^q \\ \vdots \\ \alpha_i^{q^{k-1}} \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^{r-2} c_i\alpha_i \\ \left(\sum_{i=0}^{r-2} c_i\alpha_i\right)^q \\ \vdots \\ \left(\sum_{i=0}^{r-2} c_i\alpha_i\right)^{q^{k-1}} \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

thus $\sum_{i=0}^{r-2} c_i\alpha_i \neq 0$, which implies that $\{\alpha_0, \ldots, \alpha_{r-2}\}$ is linearly independent over $\mathbb{F}_q$. Since $\mathrm{rk}_{\mathbb{F}_q}\{\alpha_0, \ldots, \alpha_{k-1}\} = r$, we assume $\{\alpha_0, \ldots, \alpha_{r-2}, \alpha_{r-1}\}$ is linear independent over $\mathbb{F}_q$ without loss of generality. Then the submatrix

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{r-1} \\ \alpha_0^q & \alpha_1^q & \ldots & \alpha_{r-1}^q \\ \vdots & \vdots & & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \ldots & \alpha_{r-1}^{q^{k-1}} \end{pmatrix}$$

of $\Delta(\alpha_0, \ldots, \alpha_{k-1})$ is with column rank $r-1$. Hence there exists $(c_0, \ldots, c_{r-1}) \in \mathbb{F}_{q^n}^{r-1} \backslash \{\mathbf{0}\}$ such that

$$\sum_{i=0}^{r-1} c_i \alpha_i^{q^j} = 0$$

for any $0 \leq j \leq k-1$. We can assume $c_{r-1} = 1$ as it is nonzero. Furthermore, since $\alpha_{r-1} \neq 0$, there exists a t, $0 \leq t \leq r-2$, such that $c_t \neq 0$. Now for any $0 \leq j \leq k-2$, we have

$$\begin{aligned} \big(\sum_{i=0}^{r-1} c_i \alpha_i^{q^j}\big)^q - \sum_{i=0}^{r-1} c_i \alpha_i^{q^{j+1}} &= \sum_{i=0}^{r-1} (c_i^q - c_i)\alpha_i^{q^{j+1}} \\ &= \sum_{i=0}^{r-2} (c_i^q - c_i)\alpha_i^{q^{j+1}}. \end{aligned}$$

Since the submatrix

$$\begin{pmatrix} \alpha_0^q & \alpha_1^q & \ldots & \alpha_{r-2}^q \\ \alpha_0^{q^2} & \alpha_1^{q^2} & \ldots & \alpha_{r-2}^{q^2} \\ \vdots & \vdots & & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \ldots & \alpha_{r-2}^{q^{k-1}} \end{pmatrix}$$

is with full column rank, we have

$$c_i^q - c_i = 0$$

for any $0 \leq i \leq r-2$. Hence $c_i \in \mathbb{F}_q$ for any $0 \leq i \leq r-1$. However, $\sum_{i=0}^{r-1} c_i\alpha_i = 0$ contradicts the fact that $\{\alpha_0, \ldots, \alpha_{r-1}\}$ is linear independent over $\mathbb{F}_q$. □

For an linearized polynomial $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathscr{L}_n(\mathbb{F}_{q^n})$ with $\mathrm{rk}\, L = k$, $0 \le k \le n$, $D_L = \begin{pmatrix} \beta_j^{q^i} \end{pmatrix} \begin{pmatrix} \alpha_i^{'q^j} \end{pmatrix} = \begin{pmatrix} \alpha_j^{q^i} \end{pmatrix} \begin{pmatrix} \beta_i^{q^j} \end{pmatrix}$ for two sets of elements $\{\alpha'_i\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$ and $\{\alpha_i\}_{i=0}^{n-1} \subseteq \mathbb{F}_{q^n}$ from Lemma 4.6, which implies that

$$
\begin{aligned}
L(x) &= (a_0, a_1, \ldots, a_{n-1}) \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \\
&= (\beta_0, \beta_1, \ldots, \beta_{n-1}) \begin{pmatrix} \alpha'_0 & \alpha_0^{'q} & \cdots & \alpha_0^{'q^{n-1}} \\ \alpha'_1 & \alpha_1^{'q} & \cdots & \alpha_1^{'q^{n-1}} \\ \vdots & \vdots & & \vdots \\ \alpha'_{n-1} & \alpha_{n-1}^{'q} & \cdots & \alpha_{n-1}^{'q^{n-1}} \end{pmatrix} \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \\
&\quad \left(= (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \begin{pmatrix} \beta_0 & \beta_0^q & \cdots & \beta_0^{q^{n-1}} \\ \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \cdots & \beta_{n-1}^{q^{n-1}} \end{pmatrix} \begin{pmatrix} x \\ x^q \\ \vdots \\ x^{q^{n-1}} \end{pmatrix} \text{ respectively } \right) \\
&= \sum_{i=0}^{n-1} \mathrm{tr}(\alpha'_i x)\beta_i \qquad \left(= \sum_{i=0}^{n-1} \mathrm{tr}(\beta_i x)\alpha_i \text{ respectively } \right).
\end{aligned}
$$

Furthermore, since $\mathrm{rk} \begin{pmatrix} \alpha_j^{'q^i} \end{pmatrix} = \mathrm{rk} \begin{pmatrix} \alpha_j^{q^i} \end{pmatrix} = \mathrm{rk}\, D_L = k$ from Remark 4.7 and Proposition 4.3, it is straightforward that $\mathrm{rk}_{\mathbb{F}_q}\{\alpha'_i\}_{i=0}^{n-1} = \mathrm{rk}_{\mathbb{F}_q}\{\alpha_i\}_{i=0}^{n-1} = k$ from Proposition 5.4. Hence Theorem 5.1(1) and 5.1(2) are obtained.

Particularly, when $k = 1$, $\mathrm{rk}_{\mathbb{F}_q}\{\alpha_i\}_{i=0}^{n-1} = 1$, so there exist c_0, c_1, $\cdots$, $c_{n-1} \in \mathbb{F}_q$ which are not all zero such that $\{\alpha_i\}_{i=0}^{n-1} = \{c_0\theta, c_1\theta, \ldots, c_{n-1}\theta\}$ for some $\theta \in \mathbb{F}_{q^n}^*$. Hence

$$
\begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^q & \alpha_1^q & \cdots & \alpha_{n-1}^q \\ \vdots & \vdots & & \vdots \\ \alpha_0^{q^{n-1}} & \alpha_1^{q^{n-1}} & \cdots & \alpha_{n-1}^{q^{n-1}} \end{pmatrix} = \begin{pmatrix} \theta \\ \theta^q \\ \vdots \\ \theta^{q^{n-1}} \end{pmatrix} (c_0, c_1, \ldots, c_{n-1})
$$

and furthermore,

$$\begin{aligned} D_L &= \begin{pmatrix} \theta \\ \theta^q \\ \vdots \\ \theta^{q^{n-1}} \end{pmatrix} (c_0, c_1, \ldots, c_{n-1}) \begin{pmatrix} \beta_0 & \beta_0^q & \cdots & \beta_0^{q^{n-1}} \\ \beta_1 & \beta_1^q & \cdots & \beta_1^{q^{n-1}} \\ \vdots & \vdots & & \vdots \\ \beta_{n-1} & \beta_{n-1}^q & \cdots & \beta_{n-1}^{q^{n-1}} \end{pmatrix} \\ &= \begin{pmatrix} \theta \\ \theta^q \\ \vdots \\ \theta^{q^{n-1}} \end{pmatrix} (\omega, \omega^q, \ldots, \omega^{q^{n-1}}) \end{aligned}$$

where $\omega = \sum_{i=0}^{n-1} c_i \beta_i$, i.e. $L(x) = \theta \mathrm{tr}(\omega x)$.

Now for any k, it is an easy exercise in linear algebra that every matrix of rank k over a field can be factorized into a sum of k matrices each of which is of rank 1 (the factorization is not necessarily unique). Hence for D_L with rank k, $0 \leq k \leq n-1$, there exist two sets of elements $\{\omega_i\}_{i=0}^{k-1} \subseteq \mathbb{F}_{q^n}$ and $\{\theta_i\}_{i=0}^{k-1} \subseteq \mathbb{F}_{q^n}$ such that

$$D_L = \sum_{i=0}^{k-1} \begin{pmatrix} \theta_i \\ \theta_i^q \\ \vdots \\ \theta_i^{q^{n-1}} \end{pmatrix} (\omega_i, \omega_i^q, \ldots, \omega_i^{q^{n-1}}),$$

which implies that $L(x) = \sum_{i=0}^{k-1} \mathrm{tr}(\omega_i x)\theta_i$. $\mathrm{rk}\,\{\omega_i\}_{i=0}^{k-1} = \mathrm{rk}\,\{\theta_i\}_{i=0}^{k-1} = k$ can be easily derived, since if not so, $L(x)$ can be represented as a sum of less than k trace terms, and hence D_L can be factorized into a sum of less than k rank 1 matrices, which contradicts $\mathrm{rk}\, D_L = k$ due to the fact that the rank of a sum of some matrices is no bigger than the sum of their ranks. Thus Theorem 5.1(3) is obtained.

5.3 Further remarks on Theorem 5.1

Now we focus on the representation of a linearized polynomial in Theorem 5.1(2). For linearized permutation polynomials, the following propositions can be easily verified.

Proposition 5.5. *(1) Assume $\{\alpha_i\}_{i=0}^{n-1}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with dual basis $\{\alpha_i^*\}_{i=0}^{n-1}$, and $L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\beta_i x)\alpha_i$. Then*

$$L^{-1}(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\alpha_i^* x)\beta_i^*;$$

(2)

$$x = \sum_{i=0}^{n-1} \mathrm{tr}(\beta_i x)\beta_i^*.$$

Proposition 5.5(2) is meaningful in understanding some concepts. For example, we always call the function $\mathrm{tr}(af(x))$, $a \in \mathbb{F}_{q^n}$, a component function of a polynomial $f(x)$ over $\mathbb{F}_{q^n}$ in cryptography. From Proposition 5.5(2), we have

$$f(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\beta_i^* f(x))\beta_i.$$

The functions $\mathrm{tr}(\beta_i^* f(x))$, $i = 0, \ldots, n-1$, are just the component functions of the map induced by $f(x)$ with respect to the basis $\{\beta_i\}_{i=0}^{n-1}$. Obviously, the so-called component functions of $f(x)$, $\mathrm{tr}(af(x))$, $a \in \mathbb{F}_{q^n}$, are just all possible $\mathbb{F}_q$-linear combinations of the component functions $\{\mathrm{tr}(\beta_i^* f(x))\}_{i=0}^{n-1}$.

Let $L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\beta_i x)\alpha_i \in \mathscr{L}_n(\mathbb{F}_{q^n})$ be a linearized polynomial of rank k. If we assume

$$(\alpha_0, \ldots, \alpha_{n-1}) = (\beta_0, \ldots, \beta_{n-1})A_L = (\beta_0^*, \ldots, \beta_{n-1}^*)B_L,$$

where A_L, $B_L \in \mathscr{M}_n(\mathbb{F}_q)$ are both of rank k. Then we can represent $L(x)$ as

$$L(x) = (\beta_0, \ldots, \beta_{n-1})A_L \begin{pmatrix} \mathrm{tr}(\beta_0 x) \\ \vdots \\ \mathrm{tr}(\beta_{n-1} x) \end{pmatrix} \tag{12}$$

or

$$L(x) = (\beta_0^*, \ldots, \beta_{n-1}^*)B_L \begin{pmatrix} \mathrm{tr}(\beta_0 x) \\ \vdots \\ \mathrm{tr}(\beta_{n-1} x) \end{pmatrix}. \tag{13}$$

These two kinds of representations for linearized polynomials are convenient when dealing with some problems. Note that

$$D_L = \left(\beta_j^{q^i}\right) A_L \left(\beta_i^{q^j}\right) = \left(\beta_j^{*q^i}\right) B_L \left(\beta_i^{q^j}\right).$$

It is easy to see from Lemma 4.2 that B_L is just the matrix of the linear transformation induced by $L(x)$ under the basis $\{\beta_i^*\}_{i=0}^{n-1}$. Hence we can easily correspond a given matrix in $\mathscr{M}_n(\mathbb{F}_q)$ to a linearized polynomial in $\mathscr{L}_n(\mathbb{F}_{q^n})$ represented in the form (13). Under this correspondence, the three kinds of elementary matrices admit three kinds of "elementary linearized polynomials" of the following form:

(1)
$$L_{ij}(x) = x - (\mathrm{tr}(\beta_i x) - \mathrm{tr}(\beta_j x))(\beta_i^* - \beta_j^*);$$

(2)
$$L_{a,i}(x) = x + a\mathrm{tr}(\beta_i x)\beta_i^*, \quad a \in \mathbb{F}_{q^n};$$

(3)
$$L_{i+j}(x) = x + \mathrm{tr}(\beta_i x)\beta_j^*.$$

From linear algebra, we know that every linearized polynomial of rank k can be represented as compositions of some elementary linearized polynomials and a linearized polynomial of the form $\sum_{i=0}^{k-1} \mathrm{tr}(\beta_i x)\beta_i^*$, which is the linearized polynomial corresponds to the matrix in the form (10).

6 Characterizations of $\mathscr{L}_n(\mathbb{F}_{q^m})$

The isomorphisms in the following theorem to characterize the subalgebra $\mathscr{L}_n(\mathbb{F}_{q^m})$ are easily to obtain.

Theorem 6.1 ([11])**.**

$$\mathscr{L}_n(\mathbb{F}_{q^m}) \cong \mathbb{F}_{q^m}[x;\sigma]/(x^n - 1) \cong \mathbb{F}_{q^m}[G].$$

Now we study the matrix of the linear transformation induced by an element of $\mathscr{L}_n(\mathbb{F}_{q^m})$. We use the notations in Section 5 and assume that $\{\beta_i\}_{i=0}^{n-1}$ is a normal basis generated by β with dual basis generator β^* here. For $L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\beta^{q^i} x)\alpha_i \in \mathscr{L}_n(\mathbb{F}_{q^m})$, we have

$$\alpha_i = L(\beta^{*q^i}), \quad 0 \le i \le n-1.$$

Assume $i = jm + k$, $j \ge 0$, $0 \le k \le m-1$. Then

$$\alpha_i = L(\beta^{*q^{jm+k}}) = \left(L(\beta^{*q^k})\right)^{q^{jm}} = \alpha_k^{q^{jm}}. \tag{14}$$

Hence the ordered set $\{\alpha_i\}_{i=0}^{n-1}$ is of the form

$$\{\alpha_0, \ldots, \alpha_{m-1}, \alpha_0^{q^m}, \ldots, \alpha_{m-1}^{q^m}, \ldots, \alpha_0^{q^{(t-1)m}}, \ldots, \alpha_{n-1}^{q^{(t-1)m}}\} \tag{15}$$

where $n = mt$. Then we have the following theorem.

Theorem 6.2. *Let V_m be the subalgebra of $\mathbb{F}_{q^n}^{\vee} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}$ formed by elements of the form*

$$\sum_{i=0}^{n-1} T_{\beta^{q^i}} \otimes \alpha_i$$

where β is a normal basis generator and $\{\alpha_i\}_{i=0}^{n-1}$ is of the form (15). Then

$$\mathscr{L}_n(\mathbb{F}_{q^m}) \cong V_m.$$

From (14), it can be checked that the matrix B_L in (13) is of the form

$$\begin{pmatrix} B_0 & B_1 & \cdots & B_{t-1} \\ B_{t-1} & B_0 & \cdots & B_{t-2} \\ \vdots & \vdots & & \vdots \\ B_1 & B_2 & \cdots & B_0 \end{pmatrix},$$

where $B_i \in \mathscr{M}_m(\mathbb{F}_q)$, $0 \leq i \leq t-1$, which is a block circulant matrix of type (t, m) [4]. Denote by $\mathscr{BC}_{t,m}(\mathbb{F}_q)$ the algebra formed by all block circulant matrices of type (t, m) over $\mathbb{F}_q$ which is a subalgebra of $\mathscr{M}_n(\mathbb{F}_q)$. The following theorem is straightforward form Theorem 2.5.

Theorem 6.3.

$$\mathscr{L}_n(\mathbb{F}_{q^m}) \cong \mathscr{BC}_{t,m}(\mathbb{F}_q).$$

Particularly, when $m = 1$, $\{\alpha_i\}_{i=0}^{n-1}$ is of the form $\{\alpha^{q^i}\}_{i=0}^{n-1}$ for some $\alpha \in \mathbb{F}_{q^n}$, and B_L is an $n \times n$ circulant matrix in this case.

Since there is a natural isomorphism between $\mathscr{BC}_{t,m}(\mathbb{F}_q)$ and $\mathscr{M}_m(\mathbb{F}_q)[x]/(x^n - 1)$ [4], and

$$\begin{aligned} \mathscr{M}_m(\mathbb{F}_q)[x]/(x^t - 1) &\cong \mathscr{M}_m(\mathbb{F}_q) \otimes_{\mathbb{F}_q} \mathbb{F}_q[x]/(x^t - 1) \\ &\cong \mathscr{M}_m\big(\mathbb{F}_q[x]/(x^t - 1)\big), \end{aligned}$$

we rediscover the following result firstly obtained by Brawley et al. in [1], through a pure matrix theoretic approach.

Corollary 6.4.

$$\mathscr{L}_n(\mathbb{F}_{q^m}) \cong \mathscr{M}_m\big(\mathbb{F}_q[x]/(x^t-1)\big).$$

It can also be checked that the matrix D_L associated to $L(x)$ is also a block circulant matrix of type (t,m). Each block of it is over $\mathbb{F}_{q^m}$, but the entries of the blocks cannot be any elements of $\mathbb{F}_{q^m}$ as there are relations between them. All the Dickson matrices associated to elements in $\mathscr{L}_n(\mathbb{F}_{q^m})$ form a $\mathbb{F}_q$-subalgebra of $\mathscr{D}_n(\mathbb{F}_{q^n})$, which is isomorphic to $\mathscr{L}_n(\mathbb{F}_{q^m})$.

Let $L(x)=\sum_{i=0}^{n-1} a_i x^{q^i} = \sum_{i=0}^{n-1} \mathrm{tr}(\beta^{q^i}x)\alpha_i$, then

$$\begin{aligned} a_i &= \sum_{l=0}^{n-1} \alpha_l \beta^{q^{i+l}} \\ &= \sum_{j=0}^{t-1} \big(\sum_{k=0}^{m-1} \alpha_k \beta^{q^{i+k}}\big)^{q^{jm}} \\ &= \mathrm{tr}_{n/m}\big(\sum_{k=0}^{m-1} \alpha_k \beta^{q^{i+k}}\big), \end{aligned}$$

where $\mathrm{tr}_{n/m}$ is the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$. Particularly, $L(x)$ can be represented as

$$L(x) = \sum_{i=0}^{n-1} \mathrm{tr}(\alpha\beta^{q^i})x^{q^i} = \sum_{i=0}^{n-1} \mathrm{tr}(\alpha^{q^{n-i}}\beta)x^{q^i}$$

for some $\alpha \in \mathbb{F}_{q^n}$ when $m=1$. We can get the following interesting property.

Proposition 6.5.

$$\mathrm{rk}_{\,\mathbb{F}_q}\{\alpha^{q^i}\}_{i=0}^{n-1} = n - \deg \gcd\big(\sum_{i=0}^{n-1} \mathrm{tr}(\alpha\beta^{q^i})x^{q^i},\ x^n-1\big),$$

where gcd *of two polynomials represents their greatest common divisor.*

7 Concluding remarks

In this paper, we propose two new characterizations of the linearized polynomial algebra $\mathscr{L}_n(\mathbb{F}_{q^n})$. The new characterizations can help us to get more

results about linearized polynomials over finite fields. As an example, we can explain the existence of some special kind of "trace representations" of linearized polynomials proposed recently and rediscover it in more simple ways. We remark that the Dickson matirx associated to a linearized polynomial is important in studying some problems, say in [9], it is used to classify equivalent classes of polynomials used in MPKC. As a result, the isomorphism we construct in Section 4 is meaningful since we can transform many problems related to linearized polynomials into matrix theoretic formats. In fact, we have used it to study quadratic exponential sums recently, but that is not a topic of this paper.

References

[1] J.V. Brawley, L. Carlitz, T. P. Vaughan, Linear permutation polynomials with coefficients in a subfield, Acta Arith. xxiv(1973) 193-199.

[2] L. Carlitz, A note on the Betti-Mathieu group, Portugal. Math. 22(1963) 121-125.

[3] P. Charpin, G. Kyureghyan, When does $G(x)+\gamma \mathrm{Tr}(H(x))$ permute $\mathbb{F}_{p^n}$?, Finite Fields Appl. 15(2009) 615C632.

[4] P. Davis, Circulant matrices, John Wiley & Sons, New York, 1979.

[5] M. Giesbrecht, Factoring in Skew-polynomial Rings over Finite Fields, J. Symbolic Computation 26(1998) 463-486.

[6] W. Greub, Multilinear algebra, second ed., Springer-Verlag, Berlin Heidelberg, 1978.

[7] N. Kolokotronis, K. Limniotis, N. Kalouptsidis, Factorization of determinants over finite fields and application in stream ciphers, Cryptogr. Commun. 1(2009) 175-205.

[8] R. Lidl, H. Niederreiter, Finite fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1997.

[9] D.D. Lin, J-C. Faugère, L. Perret, T.Z. Wang, On enumeration of polynomial equivalence classes and their application to MPKC, Finite Fields Appl. 18(2012) 283-302.

[10] S. Ling, L.J. Qu, A note on linearized polynomials and the dimension of their kernels, Finite Fields Appl. 18(2012) 56-62.

[11] B. McDonald, Finite rings with identity, Dekker, New York, 1974.

[12] C. Mortici, A basic decomposition result related to the notion of the rank of a matrix and applications, An. Şt. Univ. Ovidius Constanţa 11(2003) 125-132.

[13] O. Ore, Theory of non-commutative polynomials, Ann. of Math. 34(1933) 480-508.

[14] O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc. 35(1933) 559-584.

[15] O. Ore, Contributions to the theory of finite fields, Trans. Amer. Math. Soc. 36(1934) 243-274.

[16] K. Szymiczek, Bilinear Algebra: An Introduction to the Algebraic Theory of Quadratic Forms, Gordon and Breach Science Publishers, 1997.

[17] P.Z. Yuan, X.N. Zeng, A note on linear permutation polynomials, Finite Fields Appl. 17(2011) 488-491.

[18] K. Zhou, A remark on linear permutation polynomials, Finite Fields Appl. 14(2008) 532-536.